DEFENSE INFORMATION SYSTEMS AGENCY
STRATEGIC PLAN
2013 – 2018
VERSION 1

DISA
A COMBAT SUPPORT AGENCY

DIRECTOR'S INTENT

The Defense Information Systems Agency is at a crossroad as the Nation reflects over ten years since 9/11.

Crossroads are nothing new to the Agency — we have continually built upon a legacy of setting new standards of excellence with each opportunity to support the Warfighter. The common denominator that has been a part of each juncture has been the professional men and women of DISA . The level of excellence was present at the inception of the Defense Communications Agency during the Cold War; it was present when DISA was created in 1990. DISA's members have deployed to the edge — and are there today — as we stand shoulder to shoulder with the Warfighter no matter the location, in combat or during humanitarian assistance. DISA has risen to and met every challenge because of the ingenuity, tenacity, and recognition by our people of what it means to be a part of the Profession of Arms.

We stand shoulder to shoulder with the Warfighter, no matter the location, in combat or during humanitarian assistance.

The President, Secretary of Defense, and Chairman of the Joint Chiefs of Staff have all published their guidance and strategy for creating the military of the future. The Chairman stated, "We must develop a Joint Force for 2020 that remains ready to answer the Nation's call—anytime, anywhere. We need to offset fewer resources with more innovation." The Secretary released his strategic guidance that calls for a Joint Force of the future that will be "smaller and leaner," but also be agile, flexible, ready, and technologically advanced. "Operate Effectively in Cyberspace" is a priority and the guidance goes on to state, "Modern armed forces cannot conduct high-tempo, effective operations without reliable information and communications networks and assured access to cyberspace and space." The President stated, "As we end today's wars, we will focus on a broader range of challenges and opportunities, including the security and prosperity of the Asia Pacific."

DISA will support the Department's priority to rebalance our communications and services in the Asia-Pacific region, as well as "Operate Effectively in Cyberspace," and will play a critical role in the Department's efforts to provide modern armed forces with reliable information and communications networks and assured access to the cyber domain. DISA is a Combat Support Agency, and our number one priority is enabling information superiority for the Warfighter. We know we cannot obtain information superiority on our own, but we are proud of the capabilities we bring forward to enable the DoD to reach their goals. I intend to focus my initial efforts, in the following areas:

- ▶ Global Defense Posture
- ▶ Cyber Command and Control (C2)
- ▶ Nuclear Command, Control, and Communications (NC3)
- ▶ Joint Information Environment
- ▶ DoD Cloud Services
- ▶ Mobility
- ▶ Acquisition Agility
- ▶ DISA First

I pledge to give you my full effort to continue to make DISA the premier Combat Support Agency the Warfighter depends on to deliver capability whenever and wherever the need arises. I look forward to serving with each of you.

Ronnie D. Hawkins Jr.

RONNIE D. HAWKINS JR.
Lieutenant General, USAF
Director

THE DISA VISION

Information superiority in defense of our Nation.

THE DISA MISSION

DISA, a Combat Support Agency, provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint Warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations.

DISA's planning methodology consists of the development of three plans: The Strategic Plan, the Campaign Plan, and the Campaign Plan Implementation Plan. The DISA Strategic Plan provides a common understanding of our Agency mission and vision, and further identifies the strategic goals and key objectives that prioritize our efforts and postures the Agency for the future.

The Strategic Plan guides the development of the Campaign Plan which introduces the Agency's Lines of Operations, Joint Enablers, and specific operational initiatives that support the Agency's strategic goals. At the tactical level, the Campaign Plan Implementation Plan guides day-to-day actions and tasks and resource alignment to meet our strategic direction. These plans form our roadmap that supports the Department's vision to achieve a more effective, secure, and efficient enterprise for the DoD and the Nation.

STRATEGIC SHIFTS

Based upon recent Department of Defense Strategic Guidance, DISA is posturing to support DoD's strategic shift to rebalance global efforts towards the Asia-Pacific region and will accommodate the communications and information sharing network needs for the Joint Force of the future. As the Department evolves to meet the challenges of today's information environment, so too must DISA evolve. DISA's strategic goals are focused on the following strategic shifts:

Global Defense Posture. While maintaining our focus on the current fight in Afghanistan and our ongoing engagement efforts in Europe and Africa, we will adjust our operations to accommodate the Department's shifts in global defensive posture towards the Asia-Pacific region. We will lead the development and operation of a layered, fault-tolerant enterprise information environment consisting of rapidly deployable components that allow for contingency operations in a full range of conflict.

Cyber Command and Control (C2). We will posture the Agency in concert with U.S. Cyber Command to expand Defensive Cyber Operations (DCO) and DoD Global Information Grid Operations (DGO) mission support through evolving and innovative initiatives.

STRATEGIC SHIFTS

▶ Global Defense Posture
  ▶▶ Remain Focused on "The Fight"
  ▶▶ Rebalancing of Forces/Shift to Asia-Pacific
  ▶▶ Delivering Rapidly Deployable Solutions
▶ Cyber Command and Control (C2)
  ▶▶ Defensive Cyber Operations (DCO)
  ▶▶ DoD GIG Operations (DGO)
▶ Nuclear Command, Control, and Communications (NC3) Support
  ▶▶ Enterprise Solutions
  ▶▶ Technology Modernization
▶ DoD Joint Information Environment (JIE) Synchronization
  ▶▶ Enabling the JIE Vision
  ▶▶ JIE Technical Synchronization Office (JTSO)
▶ DoD Cloud Services
  ▶▶ Cloud Broker
  ▶▶ Cloud Infrastructure/Services
▶ Mobility Initiatives
  ▶▶ Enhanced mobile C2
  ▶▶ Secure mobile capability
▶ Acquisition Agility
  ▶▶ Enhance Enterprise Concepts
  ▶▶ Provide Agile Solutions
▶ DISA First
  ▶▶ Embrace Warfighter Needs
  ▶▶ Be the System of Choice

Nuclear Command, Control, and Communications (NC3) Support. We will focus attention on developing and enhancing enterprise solutions in support of national leadership and nuclear command and control.

DoD Joint Information Environment (JIE) Synchronization. We will be the lead for the JIE Technical Synchronization Office (JTSO). We will enable a consolidated, collaborative, and secure JIE enabling end-to-end information sharing and interdependent enterprise services across the Department.

CROSS CUTTING DISA STRATEGIC GOALS

GOAL 1 Evolve the Joint Information Environment

GOAL 2 Provide Joint C2 and Leadership Support

GOAL 3 Operate and Assure the Enterprise

GOAL 4 Optimize Department Investments

DoD Cloud Services. We will enable rapid provisioning of services for the Department as the DoD Cloud Services Broker, and we will converge components of the enterprise for a more efficient and affordable architecture through consolidation of data centers, NetOps centers, and migration to cloud computing.

Mobility Initiatives. We will promote rapid delivery, scaling, and utilization of secure mobile capability leveraging commercial mobile technology to enable an agile deployment environment for new and innovative applications to support evolving Warfighter requirements.

Acquisition Agility. DISA will employ an acquisition strategy that reduces procurement cycle times and accelerates delivery of critical capabilities. Incremental development, preplanned product improvement, and agile development will be key in our acquisition strategy.

DISA First. DISA will serve as DoD's early adopter for new enterprise capabilities. This will allow us to validate the capability meets the stated requirements, identify and resolve any issues with the capability, and demonstrate the operational viability of the capability.

THE TARGET OBJECTIVE STATE

Our target objective state is an enterprise information environment that optimizes the use of the DoD IT assets, converging communications, computing, and enterprise services into a single joint platform that can be leveraged for all Department missions. These efforts reduce total cost of ownership, reduce the attack surface of our networks, and enable DISA's mission partners to more efficiently access the information resources of the enterprise to perform their missions from any authorized IT device from anywhere in the world.

Deployed Environment

COALITION FORCES

COMPUTING   MISSION APPLICATIONS   DATA

Enterprise Information Environment

COMPUTING   APPLICATIONS   DATA

Access at the Point of Need

HOME

WORK

MOBILE (TDY/DEPLOY)

FUTURE DEVICES

OUR GUIDING PRINCIPLES

Our mission and responsibilities are global.

DISA is required to provide information at Internet speed with available and emerging technologies such that any authorized user can connect to the network with the ability to produce or consume data and services anywhere on the network globally.

Our enterprise supports the Defense Department and its mission partners.

DISA has been engaged in every mission the Department has undertaken over the decades. These engagements have become increasingly joint, interagency and international, and our partnerships have increased to reflect this.

We must support the full spectrum of operations.

The capabilities and services we provide support information sharing and facilitate decision making no matter the challenges faced and no matter where the information is located or sourced.

We operate in a contested battlespace.

Mission success is dependent upon our ability to fight through a concentrated attack while reducing the attack surface, continually improving our command and control of the network, and assuring safe, secure information sharing.

We provide integrated, interoperable, assured infrastructure, capabilities, and services that recognize the enterprise begins at the edge.

The edge is where any Warfighter or system associated with defense of our Nation is located, and we are committed to the user wherever on the globe the user operates.
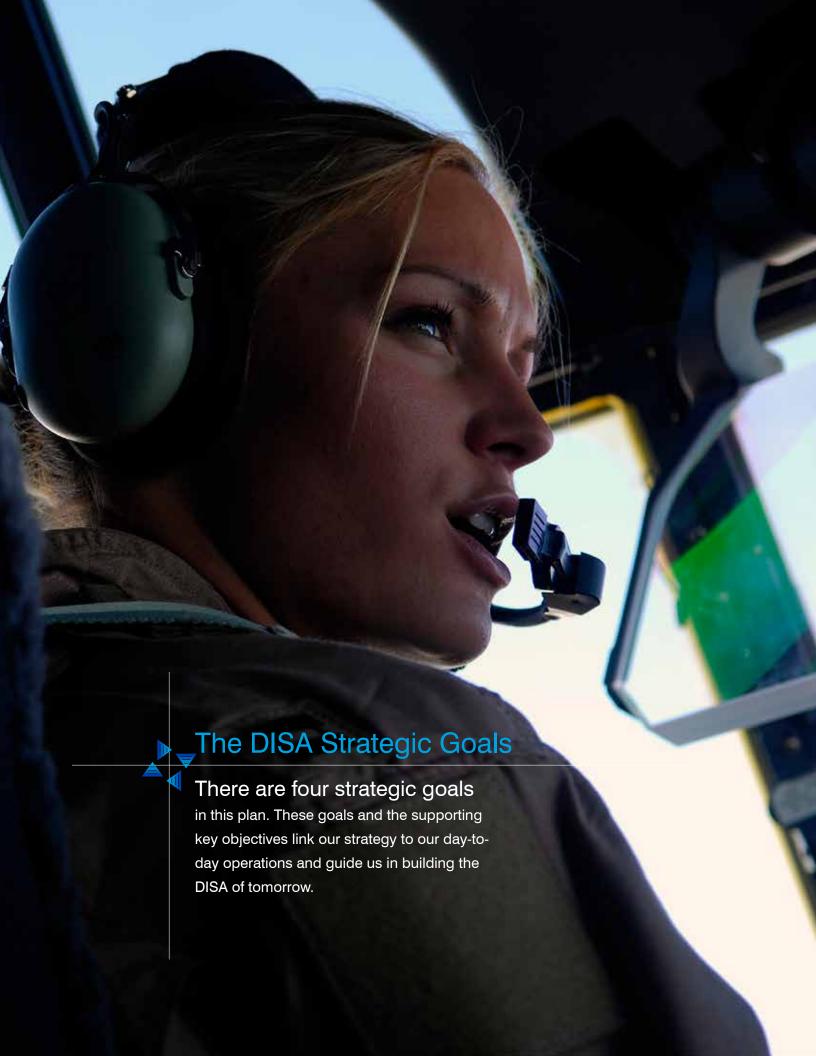
Our aim is to enable and ensure end-to-end service.

We and our mission partners are engaged from user to user – from wherever information is produced to wherever it is consumed.

The DISA enterprise must be always-on.

The capabilities and services DISA provides are expected to be on and available to users 24x7x365.

The DISA Strategic Goals

There are four strategic goals

in this plan. These goals and the supporting key objectives link our strategy to our day-to-day operations and guide us in building the DISA of tomorrow.

STRATEGIC GOAL 1

Evolve the Joint Information Environment. Evolve a consolidated, collaborative, and secure joint information environment, enabling end-to-end information sharing and interdependent enterprise services across the Department that are seamless, interoperable, efficient, and responsive to joint and coalition Warfighter requirements.

Value: Provide effective, reliable, robust capabilities that enable authorized users to connect with any device, anytime, from anywhere on the globe.

Key Objective 1.1: Implement and sustain an efficient, converged, and consolidated IT infrastructure accessible by all means from anywhere within the DoD and by any authorized user
• Converge enterprise infrastructure for a more efficient and affordable architecture through optimization and consolidation of data centers, cloud-based infrastructure, and standardized application solutions
• Lead the development and operation of a layered, fault-tolerant, rapidly restorable, enterprise information environment, with capacity on demand, consisting of rapidly deployable components that allow for contingency operations in a full range of conflict
• Deliver integrated voice, video, and/or data services ubiquitously across an interoperable, secure, and highly available IP network

infrastructure, regardless of technology, to provide increased mission effectiveness to the Warfighter
• Support the ability to rapidly deploy enterprise solutions in support of the Warfighter

Key Objective 1.2: Develop Joint Enterprise Mission Assurance Solutions that expand and extend the security protections of the Department's information assets focusing on solutions and capabilities, while enabling authorized users to productively access needed information using any device and from anywhere in DoD

Key Objective 1.3: Provide a portfolio of optimized and integrated enterprise service offerings that enable DoD-wide efficiencies and effectiveness,

and improved responsiveness to dynamic joint and coalition mission partner needs
• Optimize mission partner engagement and synchronize DISA services and capabilities to meet senior national leader, COCOM, Service, Agency, coalition, and other governmental partner mission requirements
• Drive the development of services that are standardized, common, and interoperable allowing users to access information locally and share globally across mission areas
• Deliver foundational services (i.e. metadata registry, content delivery, identity management, joint user messaging, etc) to provide a common core of infrastructure services that are critical higher level services, re-usable components and applications
• Establish a range of cloud service offerings to meet DoD requirements

Key Objective 1.4: Establish an overarching enterprise security architecture to secure and enable optimized and synchronized networks, programs, enterprise services, and joint and coalition operations

• Support command and control of the enterprise information environment by shared cyber situational awareness of the network as a whole

• Ensure protection and integrity of data in accordance with DoD-wide policies and procedures

• Enable cyber security while focusing on enhanced mobility requirements of the enterprise

• Collaborate with industry and mission partners to develop security configuration baselines for new technologies

Key Objective 1.5: Provide a full array of electromagnetic spectrum services and capabilities ranging from short notice on-the-ground operational support at the forward edge to long range planning

• Pursue national and international strategic objectives to ensure DoD's access to spectrum in support of warfighting capabilities with a view towards efficient, flexible, and adaptive technology

• Enhance quality and timeliness of operational spectrum management (SM) support for warfighting operations

• Lead the development of comprehensive and integrated strategic and implementation plans, and an architecture to transform SM to support future net-centric operations and warfare

• Perform SM and engineering analyses supporting national and international spectrum use initiatives to ensure DoD spectrum access

• Implement, integrate, and improve net-centric SM services/capabilities and influence/facilitate the implementation of emerging spectrum technologies

Key Objective 1.6: Promote rapid delivery and utilization of secure mobile capability, leveraging commercial mobile technology to enable an agile deployment environment for new and innovative applications to support evolving Warfighter requirements

• Establish common infrastructure and services for both unclassified and classified mobile solutions to enable the efficient application of mobile technologies to meet a wide range of DoD requirements

• Establish security standards and a certification process sufficiently agile to keep pace with the rate of evolving mobile technologies

• Provide a framework for management of applications to expand the capabilities available to users via mobile technology

STRATEGIC GOAL 2

Provide Joint Command and Control (JC2) and Leadership Support. Engineer, provide, and enhance command and control (C2) and mission partner information sharing capabilities to enable decision makers with the ability to exercise authority and direction over assigned and attached forces and resources while rapidly and effectively sharing information across the strategic, operational, and tactical spectrum of operations. DISA will lead the development and evolution of JC2 capabilities used to plan and execute the full range of joint, interagency, and multinational military operations.

> **Value: Deliver C2 and information sharing capabilities as a force-multiplier for the Department and national-level leaders**

Key Objective 2.1: Develop, enhance, and operate national leadership enterprise solutions
• Support national leadership and modernize as required to enable reliable nuclear command, control, and communications (NC3)
• Develop, publish, and maintain transitional architectures and standards to converge operational and strategic C2 capabilities
• Provide the ability for our national leadership to effectively coordinate, make decisions, and respond rapidly during times of stress and national emergency

Key Objective 2.2: Evolve the JC2 architecture and deploy its associated C2 enterprise capabilities
• Modernize the GCCS-J global baseline, Joint Operational Planning and Execution System (JOPES) and GCSS-J in accordance with the JC2 objective architecture
• Expand the use of widget development and delivery approach across the C2 portfolio

Key Objective 2.3: Develop and integrate material solutions as a foundation for the Future Mission Network concept
• Assist with the development of Future Mission Network operational concepts as the requirements drivers for integrated mission partner IT capabilities
• Migrate the existing Rel-Secret capabilities to a more efficient infrastructure and set of common services
• Deliver and evolve the enterprise unclassified information sharing service

STRATEGIC GOAL 3

Operate and Assure the Enterprise. Provide adaptive and innovative cyber/network command and control (C2) to enable responsive operations and defense of a joint and coalition enterprise information environment in a contested or degraded cyber battlespace ensuring information superiority in defense of our Nation across the full spectrum of military operations. Evolve our cyber and network operations capabilities to function under dynamic conditions responding to increasing Warfighter information requirements, increased demand for operational efficiencies, and shifts in the global defense posture. DISA must actualize a resilient and responsive operational structure with advanced technology, synchronized processes and procedures, and a highly-trained workforce that is prepared to consistently and rapidly adapt to changing circumstances and respond to crisis and contingency requirements around the world, on demand.

Key Objective 3.1: Operate and assure a reliable, available resilient, secure, and protected global net-centric enterprise in direct support of joint and coalition warfighting
• Execute C2 to operate and defend the DISA elements of the Global Information Grid (GIG) for networks and network services, computing, enterprise services, information assurance, senior leadership communications, C2 communications, and information sharing capabilities
• Extend DISA's operational structures to operate and defend the enterprise information environment (e.g. Joint Information Environment) and support the evolving concept of Joint Cyber Center
• Expand ability to support multiple simultaneous missions worldwide with IT capabilities

Key Objective 3.2: Ensure DISA capabilities are operated and defended; supported by life-cycle sustainment, standardization, and interoperability to achieve operational effects
• Expand NetOps governance, institutionalizing common procedures and standards for effectively inserting, operating, and defending DOTMLPF[1] capabilities in the enterprise
• Develop an operational framework to optimize service operations and provide a common understanding of how emerging technologies integrate into the enterprise
• Integrate operational readiness with Agency governance structures to inform Agency priorities of risk and associated remediation

Key Objective 3.3: Optimize mission partner engagement to anticipate, influence, and respond to DoD mission requirements
• Standardize mission partner relationship management processes to improve responsiveness to mission partners' changing requirements
• Reengineer DISA's outreach (proactive information sharing and advice) and reachback (accessibility to DISA headquarters for capabilities and services) engagement with mission partners, including evaluation of partners' operational focus (e.g. Integrated Priority Lists, OPLANs, Campaign Plans), to improve responsiveness and readiness
• Simplify provisioning Defense Enterprise Services over the DISA cloud

[1] Doctrine, Organization, Training, Materiel, Leadership, Personnel, and Facilities

Key Objective 3.4: Assess, shape, and influence the Agency's readiness posture to ensure the Agency is capable of meeting warfighting requirements

• Evolve the Agency's Readiness Program to assess the state of readiness to meet mission requirements and to know, understand, and accept risk and resource implications

• Implement a multi-faceted approach (e.g., DOTMLPF) to analyze the effectiveness of critical infrastructure and services provided to the Warfighter

• Strengthen and broaden DISA's Agency Readiness through robust engagement and participation in DoD and coalition exercises

Key Objective 3.5: Conduct, shape, and influence operational readiness, cyber risk management, and compliance processes to operate and secure the DoD enterprise infrastructure

• Develop and enforce standards and training that ensure rigorous compliance, inspections, and certification

• Foster partnerships with our mission partners, private industry, other federal departments, and our allies to exchange information and strengthen cyber security strategies

Key Objective 3.6: Evolve DISA's global NetOps structure through DOTMLPF analysis to maximize service operations, management, and mission assurance of the DISA-provided products and services, Cyber C2, and enterprise information environment

• Transform operational construct to scale for supporting growth in enterprise services across DoD organizations

• Shape and influence facility design and standardize C2 and network operations platforms globally

• Expand the DISA role in DoD-wide Defense Cyber Operations leveraging our Agency's unique joint position to create valued services, improve readiness, and enhance mission partner capabilities

• Cultivate centers of excellence in cyber and network operations

Key Objective 3.7: Adjust the Agency's capabilities to accommodate the Department's shift in global defensive posture for the 21st Century

• Plan, analyze, and assess requirements, delivering capabilities as appropriate, in support of the Department's rebalance of efforts toward the Asia-Pacific region for communications and enterprise services

• Assess and adjust capabilities to support changing needs within Europe, South-West Asia, and Afghanistan, ensuring continued support to NATO and our coalition partners

Value: Responsive operations and defense of our Warfighters' information environment

STRATEGIC GOAL 4

Optimize Department Investments. Enable the Department to maximize use of its resources by providing cost efficient capabilities; an effective and defensible infrastructure; and standardized support services, business processes, and policies that enable the rapid infusion of technology into the enterprise.

Key Objective 4.1: Promote the implementation of acquisition and procurement policies, processes, and practices that enable the development of the enterprise concept and provide agile enterprise IT contract solutions for the Department
• Support DoD efforts to develop acquisition and procurement policy enabling implementation of the enterprise information environment
• Manage or modify existing Agency contracts to eliminate duplication, optimize service offerings, and gain enterprise-level efficiencies to ensure "best value"
• Manage mission partner requirements to achieve strategic sourcing cost and performance efficiencies
• Streamline Agency acquisition and contracting processes to support the enterprise
• Support DoD CIO as the Cloud Services Broker for the Department

Key Objective 4.2: Establish and sustain a comprehensive framework to guide the development of Department systems, services, and capabilities for improved interoperability
• Leverage technical innovation and partnerships to design interoperable solutions
• Identify and integrate new information technologies into usable solutions that can be rapidly introduced and delivered
• Drive consistency for ensuring overarching security requirements are met across DoD

Key Objective 4.3: Align and prepare our workforce and DISA infrastructure to meet mission needs
• Effectively position our assets where they can be best utilized to support mission needs
• Cultivate a highly capable workforce characterized by agility, flexibility, and diversity
• Establish a strong cyber defense workforce component

Key Objective 4.4: Demonstrate fiscal responsibility in every aspect of our operations
• Ensure transparency of DISA's financial resources through clean audit opinions for the Working Capital Fund and the General Fund
• Effectively align resources to evolving mission requirements
• Implement standard business processes and models to define the enterprise capabilities and service offerings of the Agency and ensure continued value to the Department

Value: Advance mission effectiveness, achieve efficiencies, and enable the rapid infusion and integration of technology

Key Objective 4.5: Evolve the DoD's development, test, certification, deployment, and sustainment lifecycle to accelerate capability delivery and reduce lifecycle costs

• Provide the Forge.mil service to support collaborative and secure application lifecycle management

• Extend Forge.mil capabilities to include support for automated testing and certification

• Provide efficient, responsive interoperability testing, and test, evaluation, and certification (TE&C) capabilities and environments as a service

• Deliver on demand infrastructure and platform as a service (IaaS, PaaS) integrated with Forge.mil to enable continuous application delivery

Key Objective 4.6: Clearly communicate the Agency strategy, and available DISA services and capabilities, both internal and external to the Agency

• Capitalize on strategic information assets through standardized knowledge management and collaboration across the Agency and a seamless portal out to the GIG to effectively communicate with our strategic partners

• Actively engage our stakeholders, suppliers, and experts outside the Department to partner in evolving our capabilities and services to meet the needs of the Warfighter

Key Objective 4.7: Support DoD's governance of the Joint Information Environment (JIE) Initiative

• Support development of the JIE Technical Synchronization Office (JTSO)

• Provide key architectural artifacts

Key Objective 4.8: Integrate industry best practices into the existing DISA operational framework to make internal Agency interactions more efficient and improve service and responsiveness to our Agency partners

Technology for the War Fight

The services that DISA provides – communications, networking, and information services – are evolving more rapidly than almost any sector of the economy. Mobile and cloud computing technologies are globally transforming our operational landscape, enabling greater mission effectiveness through improved communication, access, information sharing, and action response time. The evolution and influx of these and other new technologies onto the commercial marketplace is occurring at an unprecedented pace. In parallel is the Warfighter's growing need for information superiority across the spectrum of operations and within the contested battlespace of the cyber domain. DISA's ability to effectively support the IT needs of the Warfighter is predicated upon our ability to keep pace with the technology within this sector.

The services that DISA provides – communications, networking, and information services – are evolving more rapidly than almost any sector of the economy.

Rapid adoption and integration of new technologies is not without challenges. Current timelines associated with certification and accreditation processes and the need for rigorous security controls must be managed. DISA will mitigate these barriers utilizing best practices to streamline business processes; anticipating the Department's demand for services and the capacity to meet those demands; and implementing a technology strategy that identifies, tracks, and plans for acquisition and integration of new technologies into the DISA catalog of services.

DISA's ability to effectively support the IT needs of the Warfighter is predicated upon our ability to keep pace with the technology within this sector.

TODAY Our talents are focused on the near-term requirements of our mission partners and the Department's vision of an enterprise information environment. At a high level:

► Converged and enhanced enterprise infrastructure
► Improved interoperability for better information sharing and collaboration
► Faster, more responsive delivery of capabilities and adoption of commercial IT
► Improved security to reduce cyber threats

TOMORROW DISA's ability to anticipate and meet the demands of our users will be based on identification and characterization of technological advancements that hold future relevance and benefit to the Department. Posturing for success, DISA has established a Strategic Technology Watchlist — a set of key focus areas identified where the associated technologies are the most critical for DISA to understand, acquire, and evolve over the next five years. DISA will effectively manage the identification, acquisition, adoption, and insertion of advanced technology into DISA systems and operations, and employ robust techniques of technology evaluation and characterization, experimentation, and piloting. The ability to conduct focused evaluations, experiments, and piloting activities is critical to the successful integration of these technologies and realization of the resulting operational capacities.

DISA Technology Watchlist for the 2013 - 2018 Strategic Plan:

High Performance Optical Networking Technologies. Refers to technologies that will allow network backbones to achieve capacity of 100 Gbps or greater. With the move to enterprise and cloud computing, improving the performance of DISA's network backbone is essential. The maturation of these technologies and the integration of the resulting capabilities are key to achieving Strategic Goal 1 (Evolve the Joint Information Environment) and Strategic Goal 3 (Operate and Assure the Enterprise).

Disruption Tolerant Networking Technologies. Refers to technologies that allow wireless networks to continue to operate effectively in the face of disruptions. In the case of SATCOM, heavy emphasis is placed on disruptions that are the result of storms, solar activity, and other environmental factors. Cyber attacks are considered the greatest threat to the DoD information systems. It is critical that DISA acquire and deploy disruption tolerant networking technology. The maturation of these technologies and the integration of the resulting capabilities are key to achieving Strategic Goal 1 (Evolve the Joint Information Environment) and Strategic Goal 3 (Operate and Assure the Enterprise).

Cloud Computing Technologies. Refers to technologies that allow service providers to provide on demand computing resources (e.g. computing capacity, storage, computing platforms, and enterprise applications) to third party consumers. As the lead provider of Cloud Computing services for the Department, DISA must acquire better technology for implementing and managing its Cloud Computing services. The maturation of these technologies and the integration of the resulting capabilities are key to achieving Strategic Goal 1 (Evolve the Joint Information Environment), Strategic Goal 2 (Provide Joint C2 and Leadership Support), Strategic Goal 3 (Operate and Assure the Enterprise), and Strategic Goal 4 (Optimize Department Investments).

Big Data Technologies. Refers to technologies for searching, mining, storing, securing, and conducting data analytics on tremendously large data sets. Big Data capabilities are becoming essential to modern warfare, and DISA needs to be able to provide Big Data capabilities to its mission partners. The maturation of these technologies and the integration of the resulting capabilities are key to achieving Strategic Goal 1(Evolve the Joint Information Environment), Strategic Goal 2 (Provide Joint C2 and Leadership Support), and Strategic Goal 3 (Operate and Assure the Enterprise).

Enterprise Management Technologies.
Refers to technologies for monitoring, managing, and protecting enterprise networks, cloud computing, and enterprise services. DISA's ability to manage its enterprise has not kept pace with the variety and scale of its enterprise services, networks, and cloud computing capabilities. New enterprise management technologies are essential. The maturation of these technologies and the integration of the resulting capabilities are key to achieving Strategic Goal 1 (Evolve the Joint Information Environment) and Strategic Goal 3 (Operate and Assure the Enterprise).

Mobile Technologies. Refers to devices and applications that are intended to be used by mobile users. The world is adopting mobile technology much more rapidly than the Department of Defense. While there are legitimate security concerns with mobile technologies, the potential operational impacts are huge. Therefore, it is critical for DISA to make inroads with mobile technologies going forward. The maturation of these technologies and the integration of the resulting capabilities are key to achieving Strategic Goal 1 (Evolve the Joint Information Environment), Strategic Goal 2 (Provide Joint C2 and Leadership Support), and Strategic Goal 3 (Operate and Assure the Enterprise).

Enterprise IdAM Technologies. Refers to the capability for (1) identifying users (people or software) that operate on the DISN and (2) managing the access of the users to network resources and services. New, more secure, and faster performance enterprise IdAM technologies are critical to DISA as the major supplier of enterprise services to the Department. The maturation of these technologies and the integration of the resulting capabilities are key to achieving the Strategic Goal 1 (Evolve the Joint Information Environment), Strategic Goal 2 (Provide Joint C2 and Leadership Support), and Strategic Goal 3 (Operate and Assure the Enterprise).
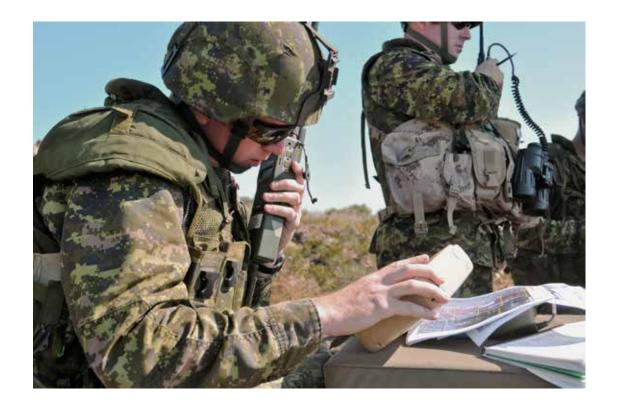
Cross Domain Technologies. Refers to technologies that allow for the safe movement of data and access of services across security enclaves. As DISA operates many security enclaves (NIPRNET, SIPRNET, and many Coalition networks) and has all of the challenges, and costs associated with multiple security enclaves, cross domain technologies are of vital importance. The maturation of these technologies and the integration of the resulting capabilities are key to achieving the Strategic Goal 1 (Evolve the Joint Information Environment), Strategic Goal 2 (Provide Joint C2 and Leadership Support), and Strategic Goal 3 (Operate and Assure the Enterprise).

These eight focus areas constitute the initial technology set for the Watchlist, and this list will be updated and evolved as the environment dictates.

BEYOND

It is imperative that we look beyond the technologies of tomorrow. We must anticipate the future capability demands of our users and how emerging technologies can be brought to bear on these critical operational challenges. Consequently, DISA must maintain a strong presence in the Science and Technology (S&T) communities, and we must effectively influence technological research and investment. This will ensure that DISA has awareness of the relevant game-changing or disruptive technologies and shape these technologies to the unique challenges of the Department of Defense. Truly disruptive technologies allow us to realize a multiplier in terms of cost savings, time savings, resource savings, or operational effectiveness. Recent examples include server virtualization, wirelessly connected tablet computers, and cloud computing.

It is imperative that we look beyond the technologies of tomorrow.

DISA's partnerships with industry, academia, and our mission partners are critical to forecasting these emerging technologies and their value to the Department, and supporting informed technology investment decisions that will strengthen the enterprise and improve the enterprise service capabilities we ultimately deliver.

Tough Choices

A comprehensive effort is required to achieve success —
accompanied by difficult choices that balance the rapid delivery of IT
capabilities and the finite resources available to support them.

These difficult choices necessitate intense scrutiny of all Agency resource
drivers, including: people, infrastructure, and programs. It is imperative that
we assess the current state of our operations, ensure we are maximizing the
efficient use of our resources to the greatest extent possible, and adjust course
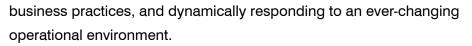where necessary.

*A comprehensive
effort is required to
achieve success
— accompanied by
difficult choices.*

People: The DISA workforce is our greatest asset. The most important factor is our ability to dynamically align and right-size DISA talent as our mission evolves. We must ultimately ensure the right technical skills and best mix of civilian, military, and contractors is available to support the Warfighter.

Infrastructure: Combining data centers and NetOps Centers to improve operational management, standardize tactics, techniques, and procedures, and reduce the total cost of ownership for the Department is inherent in our strategy. We must examine our complete global footprint, including all facilities, to determine where additional efficiencies can be gained.

We will make those tough decisions that enable us to better deliver enterprise capabilities.

Programs: Delivery and secure operation of effective IT capabilities and enterprise solutions for the Department is a critical focus area. Existing systems and capabilities must be analyzed to determine if their continuance supports our strategic direction and sunset those that do not.

As we move forward, increased attention will be paid to these areas to ensure that we are efficiently supporting the Department's joint enterprise concepts in the most cost-effective manner without sacrificing value, quality, or innovation.

We will evolve the enterprise information environment, provide joint command and control and leadership support, operate and defend the enterprise, and optimize department investments while maintaining our standard of excellence, utilizing best business practices, and dynamically responding to an ever-changing operational environment.
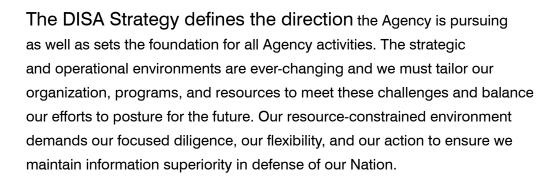
We will make those tough decisions that enable us to better deliver enterprise capabilities for the joint Warfighter, national level leadership, and mission and coalition partners, both foreign and domestic, across the range of military operations.

Conclusion

The DISA Strategy defines the direction the Agency is pursuing as well as sets the foundation for all Agency activities. The strategic and operational environments are ever-changing and we must tailor our organization, programs, and resources to meet these challenges and balance our efforts to posture for the future. Our resource-constrained environment demands our focused diligence, our flexibility, and our action to ensure we maintain information superiority in defense of our Nation.

There are Warfighters on all fronts that require DISA's continued support. As a Combat Support Agency, we know that immediate connection, sharing, and assured access to information capabilities is essential to our mission partners' operational success. Let us all embrace this imperative and evolve our capabilities to ensure secure and protected entry from every environment. We will face and adjust to the new fiscal realities before us, and we will seek optimal performance in every aspect of our operations.

We know that immediate connection, sharing, and assured access to information capabilities is essential to our mission partners' operational success.